REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of January 7, 2009 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies to Deposit Account No. 14-1437.

Claim Rejections 35 USC § 103

Claims 1 and 3 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Published Patent Application 2004/0193712 to Benenati (hereinafter Benenati) in view of U.S. Published Patent Application 2003/0014668 to Faccin, *et al.* (hereinafter Faccin), and in further view of non-patent literature reference, "A Service Framework for Carrier Grade Multimedia Services Using Parlay APIs Over a SIP System" to Pailer (hereinafter Pailer). Claim 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Benenati in view of Faccin, and further in view of Pailer.

Applicants respectfully disagree with the rejections and thus have not amended the claims. Applicants have added Claims 25-30. The added claims are fully supported by the original disclosure and no new matter has been introduced.

Aspects of Applicants' Invention

It may be helpful to reiterate certain aspects of Applicants' invention prior to addressing the cited references. One embodiment of the invention, as typified by Claim 1, is a method of authenticating a mobile communication device within a mobile network (voice network) and a wireless network (data network).

The method can include providing a mobile communication device configured to communicate over the mobile network and the wireless network, the mobile communication device including a Session Initiation Protocol (SIP) user agent executing therein; the mobile communication device receiving authentication data from a mobile service provider over the mobile network when the mobile communication device is within communication range of the mobile network; the mobile communication device building a SIP referred by token using the authentication data received from the mobile service provider; the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network.

The method also can include the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token; the SIP server sending the request for authentication of the mobile communication device to the mobile service provider; the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server; the SIP server receiving the response from the mobile service provider and sending a reply to the mobile communication device over the wireless communications link indicating whether the request for authentication was confirmed; and the mobile communication device receiving the reply from the SIP server.

See, e.g., Specification, paragraphs [0018] to [0025]; see also Fig. 2.

The Claims Define Over The Prior Art

Wireless networks are becoming increasingly prevalent with thousands of so called hotspots being deployed throughout the United States, Europe, and Asia. A hotspot refers to the coverage area surrounding a wireless access point within which a device can communicate wirelessly with the access point. The access point typically includes a wireless transceiver and is connected to a packet-switched communications network such as the Internet. As such, the access point provides network connectivity to those devices capable of establishing a wireless communications link with the access point. Mobile users can roam between multiple hot spots while maintaining connectivity with a communications network. Examples of hotspots or wireless networks can include those networks built around one of the 802 wireless communications protocols such as 802.11, 802.16, 802.20, and 802.15. Such wireless networks largely function independently of mobile communications networks. These wireless networks, particularly 802.11 wireless networks, often function purely as data networks. That is, typically voice communications are not carried over such networks. In consequence, the voice capability of mobile networks has yet to be integrated with 802.xx wireless networks. See Specification, paragraphs [0002]-[0003]. The present invention provides a method and system of authenticating a mobile communication device within a mobile network (a voice network) and a wireless network (a data network), and thus integrate these two types of networks.

Benenati discloses a method for common authentication and authorization (AA) between networks having disparate access technologies. A set of AA credentials from a user attempting to gain access to one of the networks may be received, and a subscriber database of another of the networks may be used to verify the set of AA credentials. A communication protocol common to the networks may be used. Additionally, the user may employ a single set of AA credentials, usable over multiple communication protocol layers. Further, a user may perform a single AA operation when roaming across two or more networks by gathering user's key material during an AA challenge and reply session at a data link layer. The gathered material may be used for an AA challenge at an upper network layer or another network as the user transitions between networks. See the abstract.

However, it is noted that in Benenati a set of AA credentials from a user may be used to gain access to multiple networks. In contrast, in the present invention, authentication data from a mobile service provider, not from a user, is used to gain access to a wireless network.

Benenati also does not disclose that the mobile communication device includes a Session Initiation Protocol (SIP) user agent executing therein and builds a SIP referred by token using the authentication data received from the mobile service provider. In fact, Benenati teaches away from running SIP on the user device (see paragraph [0034]: "If the user also runs IP Security (IPSec) or Session Initiation Protocol, an additional layer (Application layer) of authentication is also required. These multi-layer authentications may cause a data session to pause while the terminal is engaged in authentication requests, both upon initial connection and upon inter-technology handoff. This places a burden on the user and/or the client software and increases delays and provisioning complexities.")

Benenati further does not disclose the specific authentication steps occurred between the SIP server and the mobile service provider. More particularly, Benenati does not disclose "the mobile communication device sending the token to a SIP server via a wireless communications link over the wireless network; the SIP server interpreting the token and forming a Parlay request for authentication using data specified by the token; the SIP server sending the request for authentication of the mobile communication device to the mobile service provider; and the mobile service provider confirming or denying the request for authentication by sending a response to the SIP server," as recited in independent claims of the instant application.

In summary, since Benenati's authentication scheme is different from that of the present invention, Benenati does not disclose the specific steps or limitations recited in independent claims of the instant application.

Faccin and Pailer do not make up for the deficiencies of Benenati as discussed above. Although Faccin and Pailer mention the terms SIP protocol and Parlay respectively, they are not used in the context of present invention, namely authenticating a mobile communication device within a wireless data network using authentication data received from a mobile voice network.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claim 1, as amended. Applicants therefore respectfully submit that amended Claim 1 defines over the prior art. Furthermore, as each of the remaining claims depends from Claim 1 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Applicants thus respectfully request that the claim rejections under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

NOVAK DRUCE & QUIGG LLP

Date: April 7, 2009

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
Customer No. 40987
525 Okeechobee Boulevard, 15th Floor
West Palm Beach, FL 33401
Telephone: (561) 838-5229